

PUBLIC KEY EXCHANGE USING RIGHT TRANSVERSALS AND RIGHT LOOPS

AKHILESH CHANDRA YADAV¹ AND VIPUL KAKKAR²

ABSTRACT. In this article, we describe a key exchange protocol based on right transversals. We also describe it for general extension associated to right loops.

Keywords: Right transversals and Right loops.

Mathematical Subject Classifications: 94A60, 20N05

1. INTRODUCTION

Loops as algebraic structures had been an important object of study in mathematics starting from the first half of the 20th century with the works of Baer [3], Albert [1, 2] and Bruck [4]. It has always been practice to study right loops through its right inner mappings and inner mapping groups (also called group torsions [6]). The notion of general extension and the notion of general extension associated to a right loop has been given [6]. Indeed, it is observed that every right loop S can be embedded into a group as right transversal with some universal property [6]. The smallest subgroup generated by S is the group $G_S \times S$, the general extension associated to S . The notion of encryption and decryption has been introduced for a given right loop [10] by using bracket arrangement of weight n .

Diffie-Hellman scheme [7] is a key exchange system for establishing a common key between A and B . Their key exchange protocol is based on Cyclic groups. In 2010, M. Habeeb, D. Kahrobae, C. Koupparie and V. Spilrain introduced a new concept of key exchange protocol using semi-direct product of (semi) groups and then focused on practical instances of this general idea [5]. Their concept motivates us to give key exchange protocol based on a right transversal to a subgroup of the given group (general extensions) and general extensions associated to right loops. We also discuss key exchange protocol in the case of right gyrogroups [8] and twisted right gyrogroups [9].

2. C-GROUPOIDS AND GENERAL EXTENSIONS

A group G is called a general extension of a group H if H can be treated as a subgroup of G . Let H be a subgroup of group G . A *right transversal* to H in G is a subset S of G obtained by selecting one and only one member from each right coset of G mod H including identity e of group G . It is observed that each right transversal S to a subgroup H in a group G determines an algebraic structure (S, H, σ, f) [6] in the sense of following:

Definition 2.1. A quadruple (S, H, σ, f) , where S is a groupoid with identity e , H a group which acts on S from right through a given action θ , σ a map from S to H^H (the set of all maps from H to H) and f a map from $S \times S$ to H , is called a *c-groupoid* if it satisfies the following conditions:

- (1) $x \circ y = y \Rightarrow x = e$,
- (2) For each $x \in S, \exists x' \in S$ such that $x' \circ x = e$,

- (3) $\sigma_e = I_H$, the identity map on H , where σ_x denotes the image of x under the map σ ,
- (4) $f(x, e) = f(e, x) = 1$, the identity of H ,
- (5) $\sigma_x(h_1 h_2) = \sigma_x(h_1) \sigma_{x\theta h_1}(h_2)$,
- (6) $(x \circ y) \circ z = x\theta f(y, z) \circ (y \circ z)$,
- (7) $(x \circ y)\theta h = x\theta \sigma_y(h) \circ (y\theta h)$,
- (8) $f(x, y)f(x \circ y, z) = \sigma_x(f(y, z))f(x\theta f(y, z), y \circ z)$,
- (9) $f(x, y)\sigma_{x \circ y}(h) = \sigma_x(\sigma_y(h))f(x\theta \sigma_y(h), y\theta h)$.

where $x, y, z \in S$ and $h_1, h_2, h \in H$.

Conversely, we have

Theorem 2.2. ([6], Theorem 2.2) *Given a c-groupoid (S, H, σ, f) there is a group G which contains H as a subgroup and S as a right transversal of H in G such that the corresponding c-groupoid is (S, H, σ, f) .*

The corresponding group G is $H \times S$ together with a binary operation \cdot given by :

$$(2.1) \quad (a, x) \cdot (b, y) = (a\sigma_x(b)f(x\theta b, y), (x\theta b) \circ y).$$

This group is termed as general extension of a group H by a set S satisfying above properties (or a general extension associated to a c-groupoid).

Let (S, H, σ, f) be a c-groupoid. Let $x \in S$ and $a \in H$. Define $\beta^n(x, a)$ inductively by the following:

$$\beta^1(x, a) = x, \quad \beta^2(x, a) = x\theta a \circ x.$$

If $\beta^r(x, a)$ is defined then

$$(2.2) \quad \beta^{r+1}(x, a) = \beta^r(x, a)\theta a \circ x.$$

Similarly, we define $g^n(x, a)$ inductively by the following:

$$g^1(x, a) = a, \quad g^2(x, a) = a\sigma_x(a)f(x\theta a, x).$$

If $g^n(x, a)$ is defined, then

$$(2.3) \quad g^{n+1}(x, a) = g^n(x, a)\sigma_{\beta^n(x, a)}(a)f(\beta^n(x, a)\theta a, x)$$

Using Eqs. 2.1, 2.2, 2.3, we have

$$(2.4) \quad (a, x)^n = (g^n(x, a), \beta^n(x, a))$$

for each $n \in \mathbb{N}$.

Since

$$(a, x)^n \cdot (a, x)^m = (a, x)^{m+n} = (a, x)^m \cdot (a, x)^n$$

Using Eqns. 2.4 and 2.1, we have the following:

Lemma 2.3. *Let (S, H, σ, f) be a c-groupoid and $x \in S \setminus \{e\}, h \in H \setminus \{1\}$. Then*

(1)

$$\begin{aligned} g^{n+m}(x, a) &= g^n(x, a)\sigma_{\beta^n(x, a)}(g^m(x, a))f(\beta^n(x, a)\theta g^m(x, a), \beta^m(x, a)) \\ &= g^m(x, a)\sigma_{\beta^m(x, a)}(g^n(x, a))f(\beta^m(x, a)\theta g^n(x, a), \beta^n(x, a)) \end{aligned}$$

$$(2) \quad \beta^m(x, a)\theta g^n(x, a) \circ \beta^n(x, a) = \beta^n(x, a)\theta g^m(x, a) \circ \beta^m(x, a) = \beta^{m+n}(x, a).$$

Next, for $x \in S, a \in H$, we define $[a\sigma_x(a)]_m$ inductively by :

$$[a\sigma_x(a)]_0 = a, \quad [a\sigma_x(a)]_1 = a\sigma_x(a) \quad \text{and} \quad [a\sigma_x(a)]_n = a\sigma_x([a\sigma_x(a)]_{n-1}).$$

Then, we have the following:

Lemma 2.4. *Let (S, H, σ, f) be a c -groupoid and $x \in S \setminus \{e\}, h \in H \setminus \{1\}$. For $m \geq 2$, $\beta^m(x, a)$ is given by*

$$(2.5) \quad ((\dots (x\theta[a\sigma_x(a)]_{m-2} \circ x\theta[a\sigma_x(a)]_{m-3}) \circ \dots) \circ x\theta[a\sigma_x(a)]_0) \circ x$$

PROOF: For $m \geq 2$,

$$\begin{aligned} \beta^m(x, a) &= \{\beta^{m-1}(x, a)\theta a\} \circ x \\ &= \{(\{\beta^{m-2}(x, a)\theta a\} \circ x)\theta a\} \circ x \\ &= (\beta^{m-2}(x, a)\theta(a\sigma_x(a)) \circ x\theta a) \circ x \\ &= (\beta^{m-2}(x, a)\theta[a\sigma_x(a)]_1 \circ x\theta[a\sigma_x(a)]_0) \circ x \\ &= (((\beta^{m-3}(x, a)\theta a \circ x)\theta[a\sigma_x(a)]_1) \circ x\theta[a\sigma_x(a)]_0) \circ x \\ &= ((\beta^{m-3}(x, a)\theta(a\sigma_x([a\sigma_x(a)]_1)) \circ x\theta[a\sigma_x(a)]_1) \circ x\theta[a\sigma_x(a)]_0) \circ x \\ &= ((\beta^{m-3}(x, a)\theta([a\sigma_x(a)]_2) \circ x\theta[a\sigma_x(a)]_1) \circ x\theta[a\sigma_x(a)]_0) \circ x \\ &= \dots \quad \dots \quad \dots \\ &= \dots \quad \dots \quad \dots \\ &= [[\dots [\beta^1(x, a)\theta([a\sigma_x(a)]_{m-2}) \circ x\theta[a\sigma_x(a)]_{m-3}] \circ \dots] \circ x\theta[a\sigma_x(a)]_0] \circ x \\ &= [[\dots [x\theta([a\sigma_x(a)]_{m-2}) \circ x\theta[a\sigma_x(a)]_{m-3}] \circ \dots] \circ x\theta[a\sigma_x(a)]_0] \circ x \end{aligned}$$

□

Corollary 2.5. *If $\sigma_x = I_H$, then $[a\sigma_x(a)]_m = a^{m+1}$ and so*

$$(2.6) \quad \beta^m(x, a) = ((\dots (x\theta a^{m-1} \circ x\theta a^{m-2}) \circ \dots) \circ x\theta a) \circ x.$$

Corollary 2.6. *If $\sigma_x(h) = \eta(h)$ for all $x \in S \setminus \{e\}$ and $h \in H$, where $\eta \in \text{Aut } H$ is an involution. Then*

$$[a\sigma_x(a)]_m = \begin{cases} a[\eta(a)a]^{\frac{m}{2}} & \text{if } m \text{ is even} \\ [a\eta(a)]^{\frac{m+1}{2}} & \text{if } m \text{ is odd} \end{cases}$$

Thus

$$\beta^m(x, a) = \begin{cases} ((\dots (x\theta[a(\eta(a)a)^{\frac{m-2}{2}}] \circ x\theta[a\eta(a)]^{\frac{m-2}{2}}) \circ \dots) \circ x\theta a) \circ x & \text{if } m \text{ is even} \\ ((\dots (x\theta[a\eta(a)]^{\frac{m-1}{2}} \circ x\theta[a(\eta(a)a)^{\frac{m-3}{2}}] \circ \dots) \circ x\theta a) \circ x & \text{if } m \text{ is odd.} \end{cases}$$

3. KEY EXCHANGE PROTOCOL USING RIGHT TRANSVERSALS

Let S be a right transversal to a subgroup H in a group G . Clearly each $g \in G$ can be uniquely expressed as $g = hx$ for $h \in H$ and $x \in S$. For the sake of convenience, we shall call h as *subgroup component* of g and x as *representative* of g . Let $x \in S \setminus \{e\}$ and $a \in H \setminus \{1\}$. Keeping x and a as public, Alice chooses her private key $m \in \mathbb{N}$ and Bob chooses his private key $n \in \mathbb{N}$. Both are agree to work with the cyclic subgroup $\{(ax)^r = g^r(x, a)\beta^r(x, a); r \in \mathbb{N}\} \cup \{1e\}$. In this case the key exchange protocol is given by:

- (1) Alice computes $(ax)^m = g^m(x, a)\beta^m(x, a)$ and sends only its representative $\beta^m(x, a)$ (given by 2.4) to the Bob.
- (2) Bob computes $(ax)^n = g^n(x, a)\beta^n(x, a)$ and sends only its representative $\beta^n(x, a)$ (given by 2.4) to the Alice.

- (3) Alice computes $(\phi\beta^n(x, a)).(g^m(x, a)\beta^m(x, a))$ which is equal to

$$(\phi\sigma_{\beta^n(x, a)}f(\beta^n(x, a)\theta g^m(x, a), \beta^m(x, a))) [\beta^n(x, a)\theta g^m(x, a) o \beta^m(x, a)]$$

and her key $K_A = \beta^n(x, a)\theta g^m(x, a) o \beta^m(x, a) = \beta^{m+n}(x, a)$. Note that Alice is not able to compute subgroup component because she does not know the subgroup component $\phi = g^n(x, a)$. Thus, she computes only the representative.

- (4) Bob computes $(\psi\beta^m(x, a)).(g^n(x, a)\beta^n(x, a))$ which is equal to

$$(\psi\sigma_{\beta^m(x, a)}(g^n(x, a))f(\beta^m(x, a)\theta g^n(x, a), \beta^n(x, a))) [\beta^m(x, a)\theta g^n(x, a) o \beta^n(x, a)]$$

and his key $K_B = \beta^m(x, a)\theta g^n(x, a) o \beta^n(x, a) = \beta^{n+m}(x, a)$. Note that Bob is not able to compute subgroup component because he does not know $\psi = g^m(x, a)$. Thus, he computes only the representative.

- (5) In the general extension $G = H \times S$ determined by a c-groupoid (S, H, σ, f) ,

$$(\phi, \beta^n).(\psi, \beta^m) = (\psi, \beta^m).(\phi, \beta^n) = (a, x)^{n+m}.$$

Thus the shared common key is $K = K_A = K_B$.

4. RIGHT LOOPS AND KEY EXCHANGE PROTOCOL

A non empty set S together with binary operations o is called a *right loop* if for each $x, y \in S$, the equation $Xox = y$ has a unique solution in S . The identity element of S is denoted by e .

Let (S, o) be a right loop with identity e and y, z in S . The map $f(y, z)$ from S to S given by the equation

$$(4.1) \quad f(y, z)(x)o(yoz) = (xoy)oz, \quad x \in S$$

belongs to $Sym S$ (the Symmetric group on S) and is called a right inner mapping of (S, o) . Indeed $f(y, z) \in Sym(S \setminus \{e\}) \subseteq Sym S$. The subgroup G_S of $Sym(S \setminus \{e\}) \subseteq Sym S$ generated by $\{f(y, z) \mid y, z \in S\}$ is called the right inner mapping group (also called the group torsion [6]) of (S, o) .

Further, let $h \in Sym(S \setminus \{e\}) \subseteq Sym S$ and $y \in S$. Define $\sigma_y(h) \in Sym(S \setminus \{e\}) \subseteq Sym S$ by the equation

$$(4.2) \quad h(xoy) = \sigma_y(h)(x)oh(y), \quad x \in S$$

For the sake of convenience we shall also write $x\theta h$ for $h(x)$. Thus the equations (4.1) and (4.2) also read as

$$(4.3) \quad x\theta f(y, z)(x)o(yoz) = (xoy)oz, \quad x \in S$$

and

$$(4.4) \quad (xoy)\theta h = x\theta\sigma_y(h)oy\theta h$$

respectively.

Proposition 4.1. *Let (S, o) be a right loop with identity e . Then it determines a c-groupoid (S, G_S, σ, f) [6].*

The group $G_S \times S$ determined by c-groupoid (S, G_S, σ, f) is the smallest group generated by S , which is known as the general extension associated to the right loop S . Since all the results described as above hold in the general extension $G_S \times S$, therefore Bob and Alice may agree to work with the given right loop. Their key exchange protocol is described by the following:

Let S be a right loop and $x \in S \setminus \{e\}$ and $a \in G_S \setminus \{I_S\}$. Keeping x and a as public, Alice chooses her private key $m \in \mathbb{N}$ and Bob chooses his private key $n \in \mathbb{N}$. Both are agree to work with the cyclic subgroup $\{(a, x)^r = (g^r(x, a), \beta^r(x, a)); \mid r \in \mathbb{N}\} \cup \{(I_S, e)\}$. In this case the key exchange protocol is given by:

- (1) Alice computes $(a, x)^m = (g^m(x, a), \beta^m(x, a))$ and sends only the second component $\beta^m(x, a)$ to the Bob.
- (2) Bob computes $(a, x)^n = (g^n(x, a), \beta^n(x, a))$ and sends only the second component $\beta^n(x, a)$ to the Alice.
- (3) Alice computes $\beta^n(x, a)\theta g^m(x, a) \circ \beta^m(x, a)$. Her key is now

$$K_A = \beta^n(x, a)\theta g^m(x, a) \circ \beta^m(x, a).$$

- (4) Bob computes $\beta^m(x, a)\theta g^n(x, a) \circ \beta^n(x, a)$. His key is now

$$K_B = \beta^m(x, a)\theta g^n(x, a) \circ \beta^n(x, a).$$

- (5) Using Lemma 2.3, the shared common key $K = K_A = K_B$.

Using Lemma (2.5), we have:

Corollary 4.2. *If (S, o) is a right gyrogroup[8], then the shared common key will be $\beta^{m+n}(x, a)$, where $\beta^m(x, a) = [(\dots((x\theta a^{m-1} \circ x\theta a^{m-2})\circ x\theta a^{m-3})\dots)\circ x\theta a] \circ x$ for $m \in \mathbb{N}$.*

Corollary 4.3. *If (S, o) is a twisted right gyrogroup[9], then σ_x for every $x \in S \setminus \{e\}$, is a fixed involutory automorphism of G_S say η . In this case the shared common key will be $\beta^{n+m}(x, a)$, where $\beta^n(x, a)$ is given by Corollary 2.6.*

Example 4.4. *Let $S = \{e, x_1, x_2, \dots, x_{15}\}$. Define a binary operation o on S by taking e as the identity and defining $x_i \circ x_j = x_i$ if $i \neq j$ and $x_i \circ x_i = e$. Then (S, o) is a right loop with $x' = x$ and $f(x', x) = I_S$ for all $x \in S$. Also, for $i \neq j$*

$$x_k \theta f(x_i, x_j) = \begin{cases} x_k & \text{for } i, j \neq k \\ x_j & \text{for } k = i \\ x_i & \text{for } k = j \end{cases}$$

This shows that the group torsion $G_S = \text{Sym}(S \setminus \{e\})$. It is also evident that $f(x_i, x_j) \in \text{Aut}(S, o)$. Thus, $\text{Aut}(S, o) = G_S$ and so (S, o) is a right gyrogroup [8]. Take $x = x_3$ and $a = (x_3 \ x_4 \ x_1 \ x_9 \ x_8 \ x_7)$. Then

$$\begin{aligned} \beta^1(x, a) &= x & g^1(x, a) &= a \\ \beta^2(x, a) &= x_4 \circ x_3 = x_4 & g^2(x, a) &= a^2(x_3 \ x_4) = (x_3 \ x_1 \ x_8 \ x_4 \ x_9 \ x_7) \\ \beta^3(x, a) &= x_9 \circ x_3 = x_9 \\ g^3(x, a) &= (x_3 \ x_1 \ x_8 \ x_4 \ x_9 \ x_7) \circ a \circ (x_1 \ x_3) = (x_1 \ x_7 \ x_4 \ x_8 \ x_3 \ x_9) \end{aligned}$$

Alice chooses her private number 2 and sends $\beta^2(x, a) = x_4$ to Bob. Bob chooses his private number 3 and sends $\beta^3(x, a) = x_1$. Now, Alice computes

$$x_1 \theta g^2(x, a) \circ x_4 = x_1 \theta (x_3 \ x_1 \ x_8 \ x_4 \ x_9 \ x_7) \circ x_4 = x_8$$

and Bob computes

$$x_4 \theta g^3(x, a) \circ x_1 = x_4 \theta (x_1 \ x_7 \ x_4 \ x_8 \ x_3 \ x_9) \circ x_1 = x_8 \circ x_1 = x_8.$$

Thus their shared common key is x_8 .

REFERENCES

- [1] A. A. Albert, *Quasigroups I*, Trans. Amer. Math. Soc. **54** (1943), 507-519.
- [2] A. A. Albert, *Quasigroups II*, Trans. Amer. Math. Soc. **55** (1944), 401 -419.
- [3] R. Baer, *Nets and groups*, Trans. Amer. Math. Soc. **46** (1939), 110- 141.
- [4] R. H. Bruck, *Contributions to the theory of Loops*, Trans. Amer. Math. Soc. **60** (1946), 245- 354.
- [5] M. Habeeb, D. Kahrobaei, C. Koupparis and V. Shpilrain, *Public key exchange using semi-direct product of (semi)groups*, preprint available at <http://arxiv.org/abs/1304.6572>.

- [6] R. Lal, *Transversals in groups*, Journal of algebra, **181**(1996) 70-81.
- [7] R. Lidl and G. Pilz, *Applied Abstract Algebra*, Second edition, Springer (First Indian Reprint, 2004)
- [8] R. Lal and A. C. Yadav, *Topological right gyrogroups and gyrotransversals*, Communications in Algebra, **41(09)**(2013) 3559 - 3575.
- [9] R. Lal and A. C. Yadav, *Twisted Automorphisms and Twisted right Gyrogroups*, accepted in Communications in Algebra, estimated publication date 18 Dec, 2014(online).
- [10] A. C. Yadav, *Generating non-isomorphic right loops of a given order*, J. Disc. Math. Sci. and Cryptography, Vol. 16 (2, 3), 139-148, 2013.

¹DEPARTMENT OF MATHEMATICS, M G KASHI VIDYAPITH, VARANASI, INDIA

E-mail address, A. C. Yadav: akhileshyadav538@gmail.com

²SCHOOL OF MATHEMATICS, HARISH-CHANDRA RESEARCH INSTITUTE, ALLAHABAD, INDIA

E-mail address, V. Kakkar: vplkakk@gmail.com